

Docket No. 216642US8/btm



SO

268111
#4
7-2-02
9M

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

RECEIVED

IN RE APPLICATION OF: Shoji FUKUTOMI, et al.

GAU: 2681

MAY 24 2002

SERIAL NO: 09/996,923

EXAMINER:

Technology Center 2100

FILED: November 30, 2001

FOR: SESSION SHARED KEY SHARING METHOD, WIRELESS TERMINAL AUTHENTICATION METHOD,
WIRELESS TERMINAL AND BASE STATION DEVICE

REQUEST FOR PRIORITY

ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number [US App No], filed [US App Dt], is claimed pursuant to the provisions of 35 U.S.C. §120.
- ☐ Full benefit of the filing date of U.S. Provisional Application Serial Number, filed, is claimed pursuant to the provisions of 35 U.S.C. §119(e).
- ☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

<u>COUNTRY</u>	<u>APPLICATION NUMBER</u>	<u>MONTH/DAY/YEAR</u>
JAPAN	2000-381042	December 14, 2000
JAPAN	2001-139288	May 9, 2001

Certified copies of the corresponding Convention Application(s)

- ☒ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. filed
- ☐ were submitted to the International Bureau in PCT Application Number .
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and
(B) Application Serial No.(s)
 - ☐ are submitted herewith
 - ☐ will be submitted prior to payment of the Final Fee

RECEIVED

FEB 27 2002

Technology Center 2600



22850

Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 10/98)

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Bradley D. Lytle
Registration No. 40,073

Paul A. Sacher
Registration No. 43,418

09/996,923



日本国特許庁
JAPAN PATENT OFFICE

RECEIVED

MAY 24 2002

Technology Center 2100

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日

Date of Application:

2000年12月14日

出願番号

Application Number:

特願2000-381042

[ST.10/C]:

[JP2000-381042]

出願人

Applicant(s):

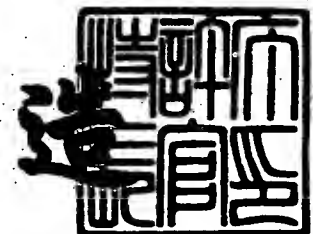
古河電気工業株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2002年 1月22日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造



【書類名】 特許願

【整理番号】 A00571

【提出日】 平成12年12月14日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 12/00
H04B 7/00

【発明者】

 【住所又は居所】 東京都千代田区丸の内2丁目6番1号 古河電気工業株式会社内

 【氏名】 福富 昌司

【発明者】

 【住所又は居所】 東京都目黒区大岡山2-12-1 東京工業大学内

 【氏名】 太田 昌孝

【特許出願人】

 【識別番号】 000005290

 【氏名又は名称】 古河電気工業株式会社

【代理人】

 【識別番号】 100089118

 【弁理士】

 【氏名又は名称】 酒井 宏明

【手数料の表示】

 【予納台帳番号】 036711

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 セッション共有鍵共有方法、無線端末認証方法、無線端末および基地局装置

【特許請求の範囲】

【請求項 1】 パケットを送受信する無線端末と該パケットを中継する基地局装置とが無線を介して通信する場合に、秘匿用および／または認証用のセッション共有鍵を前記無線端末側および前記基地局装置側に共有させるセッション共有鍵共有方法であって、

前記無線端末と前記基地局装置との通信を開始する場合に実行されるプロトコルに基づいて前記無線端末側から前記基地局装置側に対して送信されるパケットに前記セッション共有鍵の生成に用いる第 1 の情報を挿入する第 1 挿入工程と、

前記プロトコルに基づいて前記基地局装置側から前記無線端末側に対して送信されるパケットに、前記セッション共有鍵の生成に用いる第 2 の情報を挿入する第 2 挿入工程と、

前記基地局装置側で、前記第 1 挿入工程で挿入された前記第 1 の情報に基づいて前記セッション共有鍵を生成する第 1 生成工程と、

前記無線端末側で、前記第 2 挿入工程で挿入された前記第 2 の情報に基づいて前記セッション共有鍵を生成する第 2 生成工程と、

を含むことを特徴とするセッション共有鍵共有方法。

【請求項 2】 前記プロトコルは、ネットワーク層アドレスと MAC アドレスとを対応させるプロトコルであることを特徴とする請求項 1 に記載のセッション共有鍵共有方法。

【請求項 3】 前記プロトコルは、ARP であることを特徴とする請求項 1 に記載のセッション共有鍵共有方法。

【請求項 4】 前記プロトコルは、ネットワーク層アドレスを前記無線端末に割り当てるプロトコルであることを特徴とする請求項 1 に記載のセッション共有鍵共有方法。

【請求項 5】 前記プロトコルは、DHCP であることを特徴とする請求項 1 に記載のセッション共有鍵共有方法。

【請求項 6】 パケットを送受信する無線端末と該パケットを中継する基地局装置とが無線を介して通信する場合に、前記基地局装置側で前記無線端末を認証する無線端末認証方法であって、

前記認証に用いるセッション共有鍵の生成用の第 1 の情報を秘密鍵によって暗号化する暗号化工程と、

前記無線端末と前記基地局装置との通信を開始する場合に実行されるプロトコルに基づいて前記無線端末側から前記基地局装置側に対して送信されるパケットに、前記暗号化工程で暗号化された前記第 1 の情報を挿入する第 1 挿入工程と、

前記基地局装置側で、前記第 1 挿入工程で挿入された前記暗号化された第 1 の情報を、前記秘密鍵によって暗号化された情報を復号化して返信する認証局に送信し、該認証局が復号化した前記第 1 の情報を受信する復号化工程と、

前記プロトコルに基づいて前記基地局装置側から前記無線端末側に対して送信されるパケットに、前記セッション共有鍵の生成に用いる第 2 の情報を挿入する第 2 挿入工程と、

前記基地局装置側で、前記復号化工程で復号化された前記第 1 の情報に基づいて前記セッション共有鍵を生成する第 1 生成工程と、

前記無線端末側で、前記第 2 挿入工程で挿入された前記第 2 の情報に基づいて前記セッション共有鍵を生成する第 2 生成工程と、

を含むことを特徴とする無線端末認証方法。

【請求項 7】 前記プロトコルは、ネットワーク層アドレスと MAC アドレスとを対応させるプロトコルであることを特徴とする請求項 6 に記載の無線端末認証方法。

【請求項 8】 前記プロトコルは、ARP であることを特徴とする請求項 6 に記載の無線端末認証方法。

【請求項 9】 前記プロトコルは、ネットワーク層アドレスを前記無線端末に割り当てるプロトコルであることを特徴とする請求項 6 に記載の無線端末認証方法。

【請求項 10】 前記プロトコルは、DHCP であることを特徴とする請求項 6 に記載の無線端末認証方法。

【請求項 1 1】 前記第 1 の情報および前記第 2 の情報は、ディフィーヘルマン型公開鍵配送法の公開鍵であり、

前記セッション共有鍵は、ディフィーヘルマン型公開鍵配送法の共有鍵であることを特徴とする請求項 6 ～ 1 0 のいずれか一つに記載の無線端末認証方法。

【請求項 1 2】 さらに、前記無線端末側から前記基地局装置側に対して送信されるパケットのデータリンク層ペイロードおよび前記第 2 生成工程で生成された前記セッション共有鍵を含むデータに基づいてハッシュ値を算出する第 1 ハッシュ値算出工程と、

前記パケットの MAC ヘッダおよび前記ペイロードならびに前記第 1 ハッシュ値算出工程で算出された前記ハッシュ値を含むデータに基づいて CRC 値を算出する第 1 CRC 値算出工程と、

前記第 1 CRC 値算出工程で算出された前記 CRC 値を前記 MAC ヘッダおよび前記ペイロードに付加したパケットを前記無線端末側から前記基地局装置側に対して送信するパケット送信工程と、

前記基地局装置側で、前記パケット送信工程で送信された前記ペイロードおよび前記第 1 生成工程で生成された前記セッション共有鍵を含むデータに基づいてハッシュ値を算出する第 2 ハッシュ値算出工程と、

前記パケット送信工程で送信された前記 MAC ヘッダおよび前記ペイロードならびに前記第 2 ハッシュ値算出工程で算出された前記ハッシュ値を含むデータに基づいて CRC 値を算出する第 2 CRC 値算出工程と、

前記基地局装置側で、前記パケット送信工程で送信された前記 CRC 値と前記第 2 CRC 値算出工程で算出された前記 CRC 値とを比較することによって、前記無線端末をパケット単位で認証する認証工程と、

を含むことを特徴とする請求項 6 ～ 1 1 のいずれか一つに記載の無線端末認証方法。

【請求項 1 3】 パケットを中継する基地局装置と無線を介して通信する無線端末において、

前記基地局装置との通信を開始する場合に実行されるプロトコルに基づいて前記基地局装置側に対して送信するパケットに、秘匿用および／または認証用のセ

セッション共有鍵の生成に用いる第 1 の情報を挿入する挿入手段と、

前記プロトコルに基づいて前記基地局装置側から送信されるパケットに含まれる前記セッション共有鍵生成用の第 2 の情報を取得する取得手段と、

前記取得手段が取得した前記第 2 の情報に基づいて前記セッション共有鍵を生成する生成手段と、

を具備することを特徴とする無線端末。

【請求項 1 4】 パケットを中継する基地局装置と無線を介して通信する無線端末において、

当該無線端末の認証用のセッション共有鍵の生成に用いる第 1 の情報を秘密鍵によって暗号化する暗号化手段と、

前記基地局装置との通信を開始する場合に実行されるプロトコルに基づいて前記基地局装置側に対して送信するパケットに、前記暗号化手段が暗号化した前記第 1 の情報を挿入する挿入手段と、

前記プロトコルに基づいて前記基地局装置側から送信されるパケットに含まれる前記セッション共有鍵生成用の第 2 の情報を取得する取得手段と、

前記取得手段が取得した前記第 2 の情報に基づいて前記セッション共有鍵を生成する生成手段と、

を具備することを特徴とする無線端末。

【請求項 1 5】 さらに、前記基地局装置側に対して送信するパケットのデータリンク層ペイロードおよび前記生成手段が生成した前記セッション共有鍵を含むデータに基づいてハッシュ値を算出するハッシュ値算出手段と、

前記パケットの MAC ヘッダおよび前記ペイロードならびに前記ハッシュ値算出手段が算出した前記ハッシュ値を含むデータに基づいて CRC 値を算出する CRC 値算出手段と、

前記 CRC 値算出手段が算出した前記 CRC 値を前記 MAC ヘッダおよび前記ペイロードに付加したパケットを前記基地局装置側に対して送信するパケット送信手段と、

を具備することを特徴とする請求項 1 4 に記載の無線端末。

【請求項 1 6】 無線端末が送受信するパケットを中継する基地局装置にお

いて、

前記無線端末との通信を開始する場合に実行されるプロトコルに基づいて前記無線端末側から送信されるパケットに含まれ、秘匿用および／または認証用のセッション共有鍵の生成に用いる第1の情報を取得する取得手段と、

前記プロトコルに基づいて前記無線端末側に対して送信するパケットに、前記セッション共有鍵の生成に用いる第2の情報を挿入する挿入手段と、

前記取得手段が取得した前記第1の情報に基づいて前記セッション共有鍵を生成する生成手段と、

を具備することを特徴とする基地局装置。

【請求項17】 無線端末が送受信するパケットを中継する基地局装置において、

前記無線端末との通信を開始する場合に実行されるプロトコルに基づいて前記無線端末側から送信されるパケットに含まれ、秘密鍵によって暗号化された、前記無線端末の認証用のセッション共有鍵の生成に用いる第1の情報を取得する取得手段と、

前記取得手段が取得した前記暗号化された第1の情報を、前記秘密鍵によって暗号化された情報を復号化して返信する認証局に送信し、該認証局が復号化した前記第1の情報を受信する復号化手段と、

前記プロトコルに基づいて前記無線端末側に対して送信するパケットに、前記セッション共有鍵の生成に用いる第2の情報を挿入する挿入手段と、

前記復号化手段が受信した前記第1の情報に基づいて前記セッション共有鍵を生成する生成手段と、

を具備することを特徴とする基地局装置。

【請求項18】 さらに、前記無線端末側から受信したパケットのデータリンク層ペイロードおよび前記生成手段が生成した前記セッション共有鍵を含むデータに基づいてハッシュ値を算出するハッシュ値算出手段と、

前記パケットのMACヘッダおよび前記ペイロードならびに前記ハッシュ値算出手段が算出した前記ハッシュ値を含むデータに基づいてCRC値を算出するCRC値算出手段と、

前記無線端末側から受信した前記パケットのCRC値と前記CRC値算出手段が算出した前記CRC値とを比較することによって、前記無線端末をパケット単位で認証する認証手段と、

を具備することを特徴とする請求項17に記載の基地局装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

この発明は、同一データリンク層内部の無線端末および基地局装置が無線を介して通信する無線通信ネットワークシステムにおけるセッション共有鍵共有方法、無線端末認証方法、無線端末および基地局装置に関する。なお、同一データリンク層内部とは、ルータを介さずに通信することができる範囲内を意味する。

【0002】

【従来の技術】

従来、IEEE 802.11として標準化された無線LAN方式が知られている。この無線LAN方式では、アクセス方式として、CSMA/CA (Carrier Sense Multiple Access with Collision Avoid) が用いられる。また、この無線LAN方式では、通信を開始するための認証手順は特に規定されておらず、各無線端末は基本的に自由にネットワークに対するアクセスを行うことができる。

【0003】

【発明が解決しようとする課題】

しかしながら、上述した技術によれば、不正な第三者による通信の傍受や発信が容易な無線を介して無線端末側と基地局装置側との通信を行い、秘匿用および／または認証用のセッション共有鍵を無線端末側および基地局装置側に共有させる手順が規定されていないため、秘匿用および／または認証用のセッション共有鍵を無線端末側および基地局装置側に安全に共有させることができないという問題点があった。

【0004】

また、上述した技術によれば、不正な第三者による通信の傍受や発信が容易な無線を介して無線端末側と基地局装置側との通信を行い、ネットワークに接続す

る無線端末を認証するための手順が規定されていないため、ネットワークに対する不正アクセスが行われる危険性が高いという問題点があった。また、ハンドオーバーの必要があるとともにパケット落ちの確率が高い無線端末による通信を行う場合、無線端末と基地局装置との通信を開始するときのパケット交換回数を増加させると、通信確立までの遅延が増大するという不具合がある。

【0005】

この発明は上記に鑑みてなされたものであって、無線端末と基地局装置との通信確立までの遅延を抑えつつ秘匿用および／または認証用のセッション共有鍵を無線端末側および基地局装置側に安全に共有させることを第1の目的とする。また、この発明は上記に鑑みてなされたものであって、無線端末と基地局装置との通信確立までの遅延を抑えつつネットワークに対する不正アクセスを低減することを第2の目的とする。

【0006】

【課題を解決するための手段】

上記の目的を達成するために、請求項1に係るセッション共有鍵共有方法は、パケットを送受信する無線端末と該パケットを中継する基地局装置とが無線を介して通信する場合に、秘匿用および／または認証用のセッション共有鍵を前記無線端末側および前記基地局装置側に共有させるセッション共有鍵共有方法であって、前記無線端末と前記基地局装置との通信を開始する場合に実行されるプロトコルに基づいて前記無線端末側から前記基地局装置側に対して送信されるパケットに前記セッション共有鍵の生成に用いる第1の情報を挿入する第1挿入工程と、前記プロトコルに基づいて前記基地局装置側から前記無線端末側に対して送信されるパケットに、前記セッション共有鍵の生成に用いる第2の情報を挿入する第2挿入工程と、前記基地局装置側で、前記第1挿入工程で挿入された前記第1の情報に基づいて前記セッション共有鍵を生成する第1生成工程と、前記無線端末側で、前記第2挿入工程で挿入された前記第2の情報に基づいて前記セッション共有鍵を生成する第2生成工程と、を含むものである。

【0007】

この請求項1のセッション共有鍵共有方法にあっては、第1挿入工程で、無線

端末と基地局装置との通信を開始する場合に実行されるプロトコルに基づいて無線端末側から基地局装置側に対して送信されるパケットにセッション共有鍵の生成に用いる第1の情報を挿入し、第2挿入工程で、このプロトコルに基づいて基地局装置側から無線端末側に対して送信されるパケットに、セッション共有鍵の生成に用いる第2の情報を挿入し、第1生成工程で、基地局装置側で第1の情報に基づいてセッション共有鍵を生成し、第2生成工程で、無線端末側で第2の情報に基づいてセッション共有鍵を生成する。これにより、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させることなくセッション共有鍵生成用の情報を交換することができる。

【0008】

また、請求項2に係るセッション共有鍵共有方法は、請求項1に記載のセッション共有鍵共有方法において、前記プロトコルが、ネットワーク層アドレスとMACアドレスとを対応させるプロトコルであるものである。

【0009】

この請求項2のセッション共有鍵共有方法にあつては、ネットワーク層アドレスとMACアドレスとを対応させるプロトコルに基づいて基地局装置側と無線端末側との間で送受信されるパケットにセッション共有鍵生成用の情報を挿入して交換することによって、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させることなくセッション共有鍵生成用の情報を交換することができる。

【0010】

また、請求項3に係るセッション共有鍵共有方法は、請求項1に記載のセッション共有鍵共有方法において、前記プロトコルが、ARPであるものである。

【0011】

この請求項3のセッション共有鍵共有方法にあつては、ARPに基づいて基地局装置側と無線端末側との間で送受信されるパケットにセッション共有鍵生成用の情報を挿入して交換することによって、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させることなくセッション共有鍵生成用の情報を交換することができる。

【 0 0 1 2 】

また、請求項 4 に係るセッション共有鍵共有方法は、請求項 1 に記載のセッション共有鍵共有方法において、前記プロトコルが、ネットワーク層アドレスを前記無線端末に割り当てるプロトコルであるものである。

【 0 0 1 3 】

この請求項 4 のセッション共有鍵共有方法にあつては、ネットワーク層アドレスを無線端末に割り当てるプロトコルに基づいて基地局装置側と無線端末側との間で送受信されるパケットにセッション共有鍵生成用の情報を挿入して交換することによって、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させることなくセッション共有鍵生成用の情報を交換することができる。

【 0 0 1 4 】

また、請求項 5 に係るセッション共有鍵共有方法は、請求項 1 に記載のセッション共有鍵共有方法において、前記プロトコルが、DHCP であるものである。

【 0 0 1 5 】

この請求項 5 のセッション共有鍵共有方法にあつては、DHCP に基づいて基地局装置側と無線端末側との間で送受信されるパケットにセッション共有鍵生成用の情報を挿入して交換することによって、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させることなくセッション共有鍵生成用の情報を交換することができる。

【 0 0 1 6 】

また、請求項 6 に係る無線端末認証方法は、パケットを送受信する無線端末と該パケットを中継する基地局装置とが無線を介して通信する場合に、前記基地局装置側で前記無線端末を認証する無線端末認証方法であつて、前記認証に用いるセッション共有鍵の生成用の第 1 の情報を秘密鍵によって暗号化する暗号化工程と、前記無線端末と前記基地局装置との通信を開始する場合に実行されるプロトコルに基づいて前記無線端末側から前記基地局装置側に対して送信されるパケットに、前記暗号化工程で暗号化された前記第 1 の情報を挿入する第 1 挿入工程と、前記基地局装置側で、前記第 1 挿入工程で挿入された前記暗号化された第 1 の

情報を、前記秘密鍵によって暗号化された情報を復号化して返信する認証局に送信し、該認証局が復号化した前記第 1 の情報を受信する復号化工程と、前記プロトコルに基づいて前記基地局装置側から前記無線端末側に対して送信されるパケットに、前記セッション共有鍵の生成に用いる第 2 の情報を挿入する第 2 挿入工程と、前記基地局装置側で、前記復号化工程で復号化された前記第 1 の情報に基づいて前記セッション共有鍵を生成する第 1 生成工程と、前記無線端末側で、前記第 2 挿入工程で挿入された第 2 の情報に基づいて前記セッション共有鍵を生成する第 2 生成工程と、を含むものである。

【 0 0 1 7 】

この請求項 6 の無線端末認証方法にあつては、暗号化工程で、認証に用いるセッション共有鍵の生成用の第 1 の情報を秘密鍵によって暗号化し、第 1 挿入工程で、無線端末と基地局装置との通信を開始する場合に実行されるプロトコルに基づいて無線端末側から基地局装置側に対して送信されるパケットに、暗号化工程で暗号化された第 1 の情報を挿入し、復号化工程で、暗号化された第 1 の情報を基地局から認証局に送信し、該認証局が復号化した第 1 の情報を基地局で受信し、第 2 挿入工程で、このプロトコルに基づいて基地局装置側から無線端末側に対して送信されるパケットに、セッション共有鍵の生成に用いる第 2 の情報を挿入し、第 1 生成工程で、復号化工程で復号化された第 1 の情報に基づいてセッション共有鍵を生成し、第 2 生成工程で、第 2 挿入工程で挿入された第 2 の情報に基づいてセッション共有鍵を生成する。これにより、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させることなく無線端末認証用のセッション共有鍵を無線端末側および基地局装置側に安全に共有させることができる。

【 0 0 1 8 】

また、請求項 7 に係る無線端末認証方法は、請求項 6 に記載の無線端末認証方法において、前記プロトコルが、ネットワーク層アドレスと MAC アドレスとを対応させるプロトコルであるものである。

【 0 0 1 9 】

この請求項 7 の無線端末認証方法にあつては、ネットワーク層アドレスと MA

Cアドレスとを対応させるプロトコルに基づいて基地局装置側と無線端末側との間で送受信されるパケットにセッション共有鍵生成用の情報を挿入して交換することによって、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させることなく無線端末認証用のセッション共有鍵を無線端末側および基地局装置側に安全に共有させることができる。

【 0 0 2 0 】

また、請求項 8 に係る無線端末認証方法は、請求項 6 に記載の無線端末認証方法において、前記プロトコルが、A R P であるものである。

【 0 0 2 1 】

この請求項 8 の無線端末認証方法にあつては、A R P に基づいて基地局装置側と無線端末側との間で送受信されるパケットにセッション共有鍵生成用の情報を挿入して交換することによって、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させることなく無線端末認証用のセッション共有鍵を無線端末側および基地局装置側に安全に共有させることができる。

【 0 0 2 2 】

また、請求項 9 に係る無線端末認証方法は、請求項 6 に記載の無線端末認証方法において、前記プロトコルが、ネットワーク層アドレスを前記無線端末に割り当てるプロトコルであるものである。

【 0 0 2 3 】

この請求項 9 の無線端末認証方法にあつては、ネットワーク層アドレスを無線端末に割り当てるプロトコルに基づいて基地局装置側と無線端末側との間で送受信されるパケットにセッション共有鍵生成用の情報を挿入して交換することによって、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させることなく無線端末認証用のセッション共有鍵を無線端末側および基地局装置側に安全に共有させることができる。

【 0 0 2 4 】

また、請求項 1 0 に係る無線端末認証方法は、請求項 6 に記載の無線端末認証方法において、前記プロトコルが、D H C P であるものである。

【 0 0 2 5 】

この請求項 1 0 の無線端末認証方法にあつては、D H C P に基づいて基地局装置側と無線端末側との間で送受信されるパケットにセッション共有鍵生成用の情報を挿入して交換することによって、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させることなく無線端末認証用のセッション共有鍵を無線端末側および基地局装置側に安全に共有させることができる。

【 0 0 2 6 】

また、請求項 1 1 に係る無線端末認証方法は、請求項 6 ～ 1 0 のいずれか一つに記載の無線端末認証方法において、前記第 1 の情報および前記第 2 の情報が、ディフィーヘルマン型公開鍵配送法の公開鍵であり、前記セッション共有鍵が、ディフィーヘルマン型公開鍵配送法の共有鍵であるものである。

【 0 0 2 7 】

この請求項 1 1 の無線端末認証方法にあつては、ディフィーヘルマン型公開鍵配送法を用いてセッション共有鍵を無線端末側および基地局装置側に共有させることによって、セッション共有鍵をさらに適切に保護することができる。

【 0 0 2 8 】

また、請求項 1 2 に係る無線端末認証方法は、請求項 6 ～ 1 1 のいずれか一つに記載の無線端末認証方法において、さらに、前記無線端末側から前記基地局装置側に対して送信されるパケットのデータリンク層ペイロードおよび前記第 2 生成工程で生成された前記セッション共有鍵を含むデータに基づいてハッシュ値を算出する第 1 ハッシュ値算出工程と、前記パケットの M A C ヘッダおよび前記ペイロードならびに前記第 1 ハッシュ値算出工程で算出された前記ハッシュ値を含むデータに基づいて C R C 値を算出する第 1 C R C 値算出工程と、前記第 1 C R C 値算出工程で算出された前記 C R C 値を前記 M A C ヘッダおよび前記ペイロードに付加したパケットを前記無線端末側から前記基地局装置側に対して送信するパケット送信工程と、前記基地局装置側で、前記パケット送信工程で送信された前記ペイロードおよび前記第 1 生成工程で生成された前記セッション共有鍵を含むデータに基づいてハッシュ値を算出する第 2 ハッシュ値算出工程と、前記パケット送信工程で送信された前記 M A C ヘッダおよび前記ペイロードならびに前記第 2 ハッシュ値算出工程で算出された前記ハッシュ値を含むデータに基づいて C

RC値を算出する第2CRC値算出工程と、前記基地局装置側で、前記パケット送信工程で送信された前記CRC値と前記第2CRC値算出工程で算出された前記CRC値とを比較することによって、前記無線端末をパケット単位で認証する認証工程と、を含むものである。

【0029】

この請求項12の無線端末認証方法にあつては、第1ハッシュ値算出工程で、無線端末側から基地局装置側に対して送信されるパケットのデータリンク層ペイロードおよび第2生成工程で生成されたセッション共有鍵を含むデータに基づいてハッシュ値を算出し、第1CRC値算出工程で、MACヘッダおよびペイロードならびに第1ハッシュ値算出工程で算出されたハッシュ値を含むデータに基づいてCRC値を算出し、パケット送信工程で、第1CRC値算出工程で算出されたCRC値をMACヘッダおよびペイロードに付加したパケットを無線端末側から基地局装置側に対して送信し、第2ハッシュ値算出工程で、パケット送信工程で送信されたペイロードおよび第1生成工程で生成されたセッション共有鍵を含むデータに基づいてハッシュ値を算出し、第2CRC値算出工程で、パケット送信工程で送信されたMACヘッダおよびペイロードならびに第2ハッシュ値算出工程で算出されたハッシュ値を含むデータに基づいてCRC値を算出し、認証工程で、パケット送信工程で送信されたCRC値と第2CRC値算出工程で算出されたCRC値とを比較することによって、基地局側で無線端末をパケット単位で認証する。これにより、パケットのフォーマットを変更することなくパケット単位の認証を行うことができる。

【0030】

また、請求項13に係る無線端末は、パケットを中継する基地局装置と無線を介して通信する無線端末において、前記基地局装置との通信を開始する場合に実行されるプロトコルに基づいて前記基地局装置側に対して送信するパケットに、秘匿用および／または認証用のセッション共有鍵の生成に用いる第1の情報を挿入する挿入手段と、前記プロトコルに基づいて前記基地局装置側から送信されるパケットに含まれる前記セッション共有鍵生成用の第2の情報を取得する取得手段と、前記取得手段が取得した前記第2の情報に基づいて前記セッション共有鍵

を生成する生成手段と、を具備するものである。

【 0 0 3 1 】

この請求項 1 3 の無線端末にあっては、挿入手段が、基地局装置との通信を開始する場合に実行されるプロトコルに基づいて基地局装置側に対して送信するパケットに、秘匿用および／または認証用のセッション共有鍵の生成に用いる第 1 の情報を挿入し、取得手段が、このプロトコルに基づいて基地局装置側から送信されるパケットに含まれるセッション共有鍵生成用の第 2 の情報を取得し、生成手段が、取得手段が取得した第 2 の情報に基づいてセッション共有鍵を生成する。これにより、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させることなくセッション共有鍵生成用の情報を交換することができる。

【 0 0 3 2 】

また、請求項 1 4 に係る無線端末は、パケットを中継する基地局装置と無線を介して通信する無線端末において、当該無線端末の認証用のセッション共有鍵の生成に用いる第 1 の情報を秘密鍵によって暗号化する暗号化手段と、前記基地局装置との通信を開始する場合に実行されるプロトコルに基づいて前記基地局装置側に対して送信するパケットに、前記暗号化手段が暗号化した前記第 1 の情報を挿入する挿入手段と、前記プロトコルに基づいて前記基地局装置側から送信されるパケットに含まれる前記セッション共有鍵生成用の第 2 の情報を取得する取得手段と、前記取得手段が取得した前記第 2 の情報に基づいて前記セッション共有鍵を生成する生成手段と、を具備するものである。

【 0 0 3 3 】

この請求項 1 4 の無線端末にあっては、暗号化手段が、当該無線端末の認証用のセッション共有鍵の生成に用いる第 1 の情報を秘密鍵によって暗号化し、挿入手段が、基地局装置との通信を開始する場合に実行されるプロトコルに基づいて基地局装置側に対して送信するパケットに、暗号化手段が暗号化した第 1 の情報を挿入し、取得手段が、このプロトコルに基づいて基地局装置側から送信されるパケットに含まれるセッション共有鍵生成用の第 2 の情報を取得し、生成手段が、取得手段が取得した第 2 の情報に基づいてセッション共有鍵を生成する。これ

により、無線端末と基地局装置との通信を開始する場合の packets 交換回数を増加させることなく無線端末認証用のセッション共有鍵を無線端末側および基地局装置側に安全に共有させることができる。

【 0 0 3 4 】

また、請求項 1 5 に係る無線端末は、請求項 1 4 に記載の無線端末において、さらに、前記基地局装置側に対して送信する packets のデータリンク層ペイロードおよび前記生成手段が生成した前記セッション共有鍵を含むデータに基づいてハッシュ値を算出するハッシュ値算出手段と、前記 packets の MAC ヘッダおよび前記ペイロードならびに前記ハッシュ値算出手段が算出した前記ハッシュ値を含むデータに基づいて CRC 値を算出する CRC 値算出手段と、前記 CRC 値算出手段が算出した前記 CRC 値を前記 MAC ヘッダおよび前記ペイロードに付加した packets を前記基地局装置側に対して送信する packets 送信手段と、を具備するものである。

【 0 0 3 5 】

この請求項 1 5 の無線端末にあつては、ハッシュ値算出手段が、基地局装置側に対して送信する packets のペイロードおよび生成手段が生成したセッション共有鍵を含むデータに基づいてハッシュ値を算出し、CRC 値算出手段が、送信 packets の MAC ヘッダおよびペイロードならびにハッシュ値算出手段が算出したハッシュ値を含むデータに基づいて CRC 値を算出し、packets 送信手段が、CRC 値算出手段が算出した CRC 値を MAC ヘッダおよびペイロードに付加した packets を基地局装置側に対して送信する。これにより、packets のフォーマットを変更することなく packets 単位の認証を行うことができる。

【 0 0 3 6 】

また、請求項 1 6 に係る基地局装置は、無線端末が送受信する packets を中継する基地局装置において、前記無線端末との通信を開始する場合に実行されるプロトコルに基づいて前記無線端末側から送信される packets に含まれ、秘匿用および／または認証用のセッション共有鍵の生成に用いる第 1 の情報を取得する取得手段と、前記プロトコルに基づいて前記無線端末側に対して送信する packets に、前記セッション共有鍵の生成に用いる第 2 の情報を挿入する挿入手段と、前

記取得手段が取得した前記第 1 の情報に基づいて前記セッション共有鍵を生成する生成手段と、を具備するものである。

【0037】

この請求項 16 の基地局装置にあっては、取得手段が、無線端末との通信を開始する場合に実行されるプロトコルに基づいて無線端末側から送信されるパケットに含まれ、秘匿用および／または認証用のセッション共有鍵の生成に用いる第 1 の情報を取得し、挿入手段が、このプロトコルに基づいて無線端末側に対して送信するパケットに、セッション共有鍵の生成に用いる第 2 の情報を挿入し、生成手段が、取得手段が取得した第 1 の情報に基づいてセッション共有鍵を生成する。これにより、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させることなくセッション共有鍵生成用の情報を交換することができる。

【0038】

また、請求項 17 に係る基地局装置は、無線端末が送受信するパケットを中継する基地局装置において、前記無線端末との通信を開始する場合に実行されるプロトコルに基づいて前記無線端末側から送信されるパケットに含まれ、秘密鍵によって暗号化された、前記無線端末の認証用のセッション共有鍵の生成に用いる第 1 の情報を取得する取得手段と、前記取得手段が取得した前記暗号化された第 1 の情報を、前記秘密鍵によって暗号化された情報を復号化して返信する認証局に送信し、該認証局が復号化した前記第 1 の情報を受信する復号化手段と、前記プロトコルに基づいて前記無線端末側に対して送信するパケットに、前記セッション共有鍵の生成に用いる第 2 の情報を挿入する挿入手段と、前記復号化手段が受信した前記第 1 の情報に基づいて前記セッション共有鍵を生成する生成手段と、を具備するものである。

【0039】

この請求項 17 の基地局装置にあっては、取得手段が、無線端末との通信を開始する場合に実行されるプロトコルに基づいて無線端末側から送信されるパケットに含まれ、秘密鍵によって暗号化された、無線端末の認証用のセッション共有鍵の生成に用いる第 1 の情報を取得し、復号化手段が、取得手段が取得した暗号

化された第1の情報を、この秘密鍵によって暗号化された情報を復号化して返信する認証局に送信し、該認証局が復号化した第1の情報を受信し、挿入手段が、このプロトコルに基づいて無線端末側に対して送信するパケットに、セッション共有鍵の生成に用いる第2の情報を挿入し、生成手段が、復号化手段が受信した第1の情報に基づいてセッション共有鍵を生成する。これにより、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させることなく無線端末認証用のセッション共有鍵を無線端末側および基地局装置側に安全に共有させることができる。

【0040】

また、請求項18に係る基地局装置は、請求項17に記載の基地局装置において、さらに、前記無線端末側から受信したパケットのデータリンク層ペイロードならびに前記生成手段が生成した前記セッション共有鍵を含むデータに基づいてハッシュ値を算出するハッシュ値算出手段と、前記パケットのMACヘッダおよび前記ペイロードならびに前記ハッシュ値算出手段が算出した前記ハッシュ値を含むデータに基づいてCRC値を算出するCRC値算出手段と、前記無線端末側から受信した前記パケットのCRC値と前記CRC値算出手段が算出した前記CRC値とを比較することによって、前記無線端末をパケット単位で認証する認証手段と、を具備するものである。

【0041】

この請求項18の基地局装置にあつては、ハッシュ値算出手段が、無線端末側から受信したパケットのデータリンク層ペイロードおよび生成手段が生成したセッション共有鍵を含むデータに基づいてハッシュ値を算出し、CRC値算出手段が、このパケットのMACヘッダおよびペイロードならびにハッシュ値算出手段が算出したハッシュ値を含むデータに基づいてCRC値を算出し、認証手段が、無線端末側から受信したパケットのCRC値とCRC値算出手段が算出したCRC値とを比較することによって、無線端末をパケット単位で認証する。これにより、パケットのフォーマットを変更することなくパケット単位の認証を行うことができる。

【0042】

【発明の実施の形態】

以下に、この発明の実施の形態を、添付の図面を参照して詳細に説明する。なお、この実施の形態によってこの発明が限定されるものではない。

【0043】

図1は、この発明の一実施の形態にかかる通信ネットワークシステムの構成を示す説明図である。この通信ネットワークシステムは、バックボーンネットワーク43と、バックボーンネットワーク43とインターネット1とを接続するルータ2と、事業者ごとの広域LAN10-1～10-N1と、各広域LAN10-1～10-N1をバックボーンネットワーク43にそれぞれ接続するルータ3-1～3-N1とを備える。各広域LAN10-1～10-N1には、少なくとも一つの基地局（アクセスポイント）がそれぞれ接続されている。この例では、広域LAN10-1には、アクセスポイント4-1～4-N2が接続され、広域LAN10-N1には、アクセスポイント6-1～6-N3が接続されている。

【0044】

各アクセスポイントは、無線端末と無線を介して接続され、無線ネットワークを形成する。この例では、アクセスポイント4-1は、無線端末8-1～8-k1と接続され、無線ネットワーク41-1を形成している。また、アクセスポイント4-N2は、無線端末8-k2～8-N4と接続され、無線ネットワーク41-N2を形成している。また、アクセスポイント6-1は、無線端末9-1～9-k3と接続され、無線ネットワーク42-1を形成している。また、アクセスポイント6-N3は、無線端末9-k4～9-N5と接続され、無線ネットワーク42-N3を形成している。各無線端末は、アクセスポイントを介してインターネット1や他の無線端末との通信を行うことができる。

【0045】

また、各広域LAN10-1～10-N1には、無線端末の認証データを保持する認証サーバ5-1～5-N1がそれぞれ接続されている。認証サーバ5-1～5-N1は、各アクセスポイントと信頼性のある通信を行うことができる。各無線端末のユーザは、いずれかの事業者と、その事業者のネットワークを利用する契約を交わしている。各認証サーバ5-1～5-N1は、自認証サーバを有す

る事業者（以下、自事業者と呼ぶ）と契約したユーザ（以下、契約ユーザと呼ぶ）の無線端末を認証する認証データを保持している。ここで、認証データとは、ユーザのIDおよびユーザと共有する秘密鍵である。

【0046】

なお、鍵とは、情報を暗号化および／または復号化する情報のことである。また、ルータ2および3-1～3-N1に代えてブリッジを用いてもよい。また、各認証サーバ5-1～5-N1は、各広域LAN10-1～10-N1に直接接続されていなくてもよく、たとえば、インターネット1等に接続され、各ルータ3-1～3-N1を介して各広域LAN10-1～10-N1に接続されるようにしてもよい。

【0047】

つぎに、無線端末の構成について説明する。図2は、図1に示した無線端末8-1の概略構成を示すブロック図である。無線端末8-1は、ユーザのIDおよび秘密鍵ならびにディフィーヘルマン型公開鍵配送法に用いる素数 p および原始根 α の情報を保持する記憶装置11と、ディフィーヘルマン型公開鍵配送法に基づいて、素数 p および原始根 α を用いて公開鍵 Y_A を生成し、アクセスポイントからの公開鍵 Y_B を取得し、セッション共有鍵 K を算出して記憶装置11に格納するディフィーヘルマン計算部13と、ディフィーヘルマン計算部13が生成した公開鍵 Y_A を秘密鍵で暗号化する暗号化部15とを備える。

【0048】

また、無線端末8-1は、アクセスポイントとの通信を開始する場合、DHCP (Dynamic Host Configuration Protocol) に基づくパケットの送受信を行うDHCP処理部16と、送信するパケットのデータリンク層ペイロードおよびセッション共有鍵 K を含むデータに基づいてハッシュ値を算出するハッシュ値計算部12と、送信するパケットのデータリンク層ペイロードおよびMACアドレスならびにハッシュ値計算部12が算出したハッシュ値を含むデータに基づいてCRC値を算出するCRC値計算部14と、MACフレームの送受信処理を行うパケット処理部17と、無線を介してアクセスポイントと通信する無線通信部18とを備える。

【 0 0 4 9 】

素数 p および原始根 α は、あらかじめ、各無線端末と各アクセスポイントとで共有されている。たとえば、原始根 α として「2」を用い、素数 p として 7 6 8 ビットや 1 0 2 4 ビットの素数を用いる。記憶装置 1 1 は、EEPROM や電源バックアップされた RAM 等の書き込み可能な不揮発性記録媒体を有し、ID, 秘密鍵, 素数 p および原始根 α の情報を保持する。ディフィーヘルマン計算部 1 3 は、ディフィーヘルマン型公開鍵配送法に基づいて、 $[0, p - 1]$ の間の整数 X_A をランダムに選び、記憶装置 1 1 に保持された素数 p および原始根 α の情報ならびに整数 X_A を用いて公開鍵 Y_A を生成し、アクセスポイントからの公開鍵 Y_B を取得し、整数 X_A および公開鍵 Y_B を用いてセッション共有鍵 K を算出し、記憶装置 1 1 に格納する。

【 0 0 5 0 】

暗号化部 1 5 は、ディフィーヘルマン計算部 1 3 が生成した公開鍵 Y_A を、記憶装置 1 1 に保持された秘密鍵で暗号化する。DHCP 処理部 1 6 は、DHCP に基づいて送信する DHCP-DISCOVER や DHCP-REQUEST 等の所定の packets に、記憶装置 1 1 に記憶された ID および暗号化部 1 5 が暗号化した公開鍵 Y_A (以下、暗号化された公開鍵 Y_A を $E(Y_A)$ と記す) を挿入する。この挿入は、packet の MAC ヘッダ部分に行ってもよいし、データリンク層ペイロード部分に行ってもよい。また、DHCP 処理部 1 6 は、アクセスポイントから DHCP に基づいて送信される DHCP-OFFER や DHCP-ACK 等の所定の packet を取得し、この packet に含まれる公開鍵 Y_B を抽出してディフィーヘルマン計算部 1 3 に出力する。

【 0 0 5 1 】

ハッシュ値計算部 1 2 は、送信する packet のデータリンク層ペイロードおよび記憶装置 1 1 に保持されたセッション共有鍵 K を含むデータに基づいてハッシュ値を算出する。CRC 値計算部 1 4 は、送信する packet のデータリンク層ペイロードおよび MAC アドレスならびにハッシュ値計算部 1 2 が算出したハッシュ値を含むデータに基づいて CRC 値を算出する。packet 処理部 1 7 は、データリンク層ペイロードおよび MAC アドレスならびに CRC 値計算部 1 4 が算出

したCRC値からMACフレームを生成して送信し、また、アクセスポイントからのMACフレームを受信する。

【0052】

無線通信部18は、無線を介してアクセスポイントと通信する。無線端末8-1は、そのユーザと契約している事業者のアクセスポイント4-1~4-N2にアクセスできるとともに、ローミングによって、アクセスポイント6-1~6-N3等の他の事業者のアクセスポイントに対するアクセスを行うことができる。ローミングの場合、アクセス先のネットワークの認証サーバから認証サーバ5-1に対して $E(Y_A)$ およびIDが送信され、認証サーバ5-1は、復号化した公開鍵 Y_A を返信する。他の各無線端末も無線端末8-1と同じ構成を有する。

【0053】

つぎに、アクセスポイントについて説明する。図3は、図1に示したアクセスポイント4-1の概略構成を示すブロック図である。アクセスポイント4-1は、広域LAN10-1との通信を行うLAN通信部21と、素数 p 、原始根 α 、認証サーバのアドレスおよびDHCPサーバのアドレスの情報を保持する記憶装置22と、ディフィーヘルマン型公開鍵配送法に基づいて、無線端末からの公開鍵 Y_A を取得し、素数 p および原始根 α を用いて公開鍵 Y_B を生成し、セッション共有鍵 K を算出して記憶装置22に格納するディフィーヘルマン計算部24とを備える。

【0054】

また、アクセスポイント4-1は、DHCPに基づく所定の packets を検出し、ディフィーヘルマン型公開鍵配送法の公開鍵の抽出および挿入を行うDHCP処理部23と、無線端末からの packets のデータリンク層ペイロードおよびセッション共有鍵 K を含むデータに基づいてハッシュ値を算出し、この packets のデータリンク層ペイロードおよびMACアドレスならびに算出したハッシュ値を含むデータに基づいてCRC値を算出するハッシュ値/CRC値計算部26と、MACフレームの送受信処理を行うとともに無線端末の packets ごとの認証を行う packets 処理部25と、無線を介して無線端末と通信する無線通信部27とを備

える。

【0055】

LAN通信部21は、広域LAN10-1との通信を行う。記憶装置22は、ハードディスクやRAM等の記録媒体を有し、素数 p 、原始根 α 、認証サーバのアドレスおよびDHCPサーバのアドレスの情報を保持する。ディフィーヘルマン計算部24は、ディフィーヘルマン型公開鍵配送法に基づいて、無線端末からの公開鍵 Y_A を取得し、 $[0, p-1]$ の間の整数 X_B をランダムに選び、記憶装置22に保持された素数 p および原始根 α ならびに整数 X_B を用いて公開鍵 Y_B を生成し、整数 X_B および公開鍵 Y_A を用いてセッション共有鍵 K を算出して記憶装置22に格納する。

【0056】

DHCP処理部23は、パケット処理部25からのパケットをLAN通信部21に転送するとともにLAN通信部21からのパケットをパケット処理部25に転送する。そして、DHCP処理部23は、パケット処理部25からLAN通信部21に転送するパケットをチェックして、 $E(Y_A)$ およびIDの情報を含むDHCPに基づく所定のパケットを検出し、このパケットに含まれる $E(Y_A)$ およびIDを抽出し、認証サーバ5-1に送信して復号化を依頼し、認証サーバ5-1からの復号化された公開鍵 Y_A を受信する。

【0057】

また、DHCP処理部23は、LAN通信部21からパケット処理部25に転送するパケットをチェックして、DHCPに基づく所定のパケットを検出し、このパケットに、ディフィーヘルマン計算部24が算出した公開鍵 Y_B を挿入してパケット処理部25に転送する。ハッシュ値/CRC値計算部26は、無線端末からのパケットのデータリンク層ペイロードおよび記憶装置22に保持されセッション共有鍵 K を含むデータに基づいてハッシュ値を算出し、このパケットのデータリンク層ペイロードおよびMACアドレスならびに算出したハッシュ値を含むデータに基づいてCRC値を算出する。

【0058】

パケット処理部25は、MACフレームの送受信処理を行うとともに、内蔵す

る認証部 2 8 によってパケットごとの無線端末の認証を行う。認証部 2 8 は、無線端末からのパケットの CRC 値とハッシュ値 / CRC 値計算部 2 6 が算出した CRC 値とを比較し、一致するか否かに基づいて正当なアクセスであるか不正なアクセスであるかを判定し、不当なアクセスである場合は、そのパケットを破棄する。あるいは、通信の乱れによるデータエラーを考慮して、パケットの再送要求を行ってもよい。無線通信部 2 7 は、無線を介して各無線端末と通信する。

【 0 0 5 9 】

なお、ここでは、認証サーバ 5 - 1 が DHCP サーバを兼ねる例を示すので、記憶装置 2 2 には、認証サーバ 5 - 1 のアドレスの情報と DHCP サーバのアドレスの情報をまとめて保持する。また、DHCP 処理部 2 3 が、認証サーバ 5 - 1 宛ての DHCP に基づく所定のパケットをそのまま転送し、認証サーバ 5 - 1 が、このパケットから $E(Y_A)$ および ID を抽出し、復号化した公開鍵 Y_A を DHCP に基づく所定のパケットとともにアクセスポイント 4 - 1 に送信してもよい。他のアクセスポイントもアクセスポイント 4 - 1 と同じ構成を有する。

【 0 0 6 0 】

つぎに、認証サーバについて説明する。図 4 は、図 1 に示した認証サーバ 5 - 1 の概略構成を示すブロック図である。認証サーバ 5 - 1 は、自事業者の各契約ユーザの秘密鍵および ID の情報および DHCP 用のデータを保持する記憶装置 3 1 と、アクセスポイントによって送信されてきた ID に応じた秘密鍵でアクセスポイントによって送信されてきた $E(Y_A)$ を復号化して返信する復号化部 3 2 と、DHCP の送受信処理を行う DHCP 処理部 3 3 と、広域 LAN 1 0 - 1 との通信を行う LAN 通信部 3 4 とを備える。

【 0 0 6 1 】

記憶装置 3 1 は、ハードディスクや RAM 等の記録媒体を有し、自事業者の各契約ユーザの秘密鍵および ID の情報および DHCP 用のデータを保持する。復号化部 3 2 は、アクセスポイントによって送信されてきた ID に応じた秘密鍵でアクセスポイントによって送信されてきた $E(Y_A)$ を復号化し、送信元のアクセスポイントに返信する。また、アクセスポイントによって送信されてきた ID が他の事業者の ID であって、ローミングが可能な場合は、該他の事業者の認証

サーバに該IDおよびE(Y_A)を送信して復号化を依頼する。

【0062】

このように、E(Y_A)の復号化は、公開鍵Y_Aを暗号化したユーザと契約した事業者の認証サーバのみによって行われるため、他の事業者が有するローミング先の認証サーバや、情報が盗難される危険性の高いアクセスポイントに秘密鍵を渡す必要がない。すなわち、秘密鍵を適切に保護することができる。DHCP処理部33は、DHCP-DISCOVERやDHCP-REQUEST等のパケットを受信し、DHCP-OFFERやDHCP-ACK等のパケットを送信して、IPアドレスを無線端末に動的に割り当てるDHCP処理を行う。LAN通信部34は、広域LAN10-1との通信を行う。

【0063】

なお、ここでは、認証サーバ5-1がDHCPサーバを兼ねる例を示したが、認証サーバ5-1とは別にDHCPサーバを設けてもよい。また、各アクセスポイント4-1~4-N2がDHCPサーバを兼ねてもよい。この場合は、各アクセスポイント4-1~4-N2のDHCP処理部23が、認証サーバ5-1が実行していたDHCP処理を実行する。他の認証サーバ5-2~5-N1も認証サーバ5-1と同じ構成を有する。

【0064】

また、前述した無線端末、アクセスポイントおよび認証サーバの各構成要素は、機能概念的なものであり、必ずしも物理的に図示したように構成されていなくてもよい。たとえば、これら各構成要素が備える処理機能のうち全部または一部を、図示しないCPU (Central Processing Unit) およびこのCPUにて解釈実行されるプログラムによって実現することができる。すなわち、図示しないROMには、OS (Operating System) 等と協働してCPUに命令を与え、CPUに各種処理を行わせるコンピュータプログラムが格納されている。そして、CPUは、このプログラムに従って各種処理を行う。また、これら各構成要素が備える処理機能のうち全部または一部を、ワイヤードロジックによるハードウェアとして実現することも可能である。

【0065】

つぎに、この実施の形態の動作について図5～図9を参照して説明する。図5は、この実施の形態にかかる、通信に先立ってセッション共有鍵Kを生成するセッション共有鍵生成処理の処理手順を示す説明図である。ここでは、無線端末8-1およびアクセスポイント4-1がセッション共有鍵Kを生成する場合を例に挙げる。このセッション共有鍵生成処理では、まず、無線端末8-1が、整数 X_A を決定して記憶する(S1)。つぎに、無線端末8-1は、素数 p 、原始根 α および整数 X_A に基づいて、式1で示される公開鍵 Y_A を算出する(S2)。

$$Y_A = \alpha^{(X_A)} \bmod (p) \quad \cdots \text{(式1)}$$

ただし、 $A \bmod (B)$ は、整数Aを整数Bによって除算した余りを示し、 A^B は、AのB乗を示す。

【0066】

つぎに、無線端末8-1は、算出した公開鍵 Y_A を秘密鍵によって暗号化して $E(Y_A)$ を生成し(S3)、IDおよび $E(Y_A)$ をDHCP-REQUESTに挿入してアクセスポイント4-1に送信する(S4)。アクセスポイント4-1は、DHCP-REQUESTを受信すると、このDHCP-REQUESTを転送するとともに、このDHCP-REQUESTに含まれるIDおよび $E(Y_A)$ を抽出し、このIDおよび $E(Y_A)$ を認証サーバ5-1に送信して $E(Y_A)$ の復号化を依頼する(S5)。認証サーバ5-1は、DHCP-REQUESTならびにIDおよび $E(Y_A)$ を受信すると、このIDに対応する秘密鍵によって $E(Y_A)$ を復号化し、復号化した公開鍵 Y_A を、DHCP-ACKとともにアクセスポイント4-1に返信する(S6)。

【0067】

アクセスポイント4-1は、DHCP-ACKおよび公開鍵 Y_A を受信すると、整数 X_B を決定する(S7)。つぎに、アクセスポイント4-1は、素数 p 、原始根 α および整数 X_B に基づいて、式2で示される公開鍵 Y_B を算出する(S8)。

$$Y_B = \alpha^{(X_B)} \bmod (p) \quad \cdots \text{(式2)}$$

つぎに、アクセスポイント4-1は、公開鍵 Y_B をDHCP-ACKに挿入して無線端末8-1に送信する(S9)。また、アクセスポイント4-1は、公開

鍵 Y_A および整数 X_B に基づいて、式 3 で示されるセッション共有鍵 K を算出して記憶する (S10)。

【0068】

$$K = Y_A^{X_B} \bmod (p) = \alpha^{(X_A \cdot X_B)} \bmod (p) \quad \dots (式3)$$

一方、無線端末 8-1 は、DHCP-ACK を受信すると、DHCP-ACK に含まれる公開鍵 Y_B を抽出する。そして、無線端末 8-1 は、公開鍵 Y_B および整数 X_A に基づいて、式 4 で示されるセッション共有鍵 K を算出して記憶する (S11)。

$$K = Y_B^{X_A} \bmod (p) = \alpha^{(X_A \cdot X_B)} \bmod (p) \quad \dots (式4)$$

【0069】

ここで、アクセスポイント 4-1 と無線端末 8-1 とが正しくセッション共有鍵 K を共有できた場合は、無線端末 8-1 と認証サーバ 5-1 とが秘密鍵を共有しているということがいえるので、アクセスポイント 4-1 は、無線端末 8-1 が正当な無線端末であることを認証することができる。逆に、アクセスポイント 4-1 と無線端末 8-1 とが正しくセッション共有鍵 K を共有できなかった場合は、無線端末 8-1 と認証サーバ 5-1 とが秘密鍵を共有していないということがいえるので、アクセスポイント 4-1 は、無線端末 8-1 が不正な無線端末であると判断することができる。

【0070】

このように、セッション共有鍵 K を生成するための公開鍵 Y_A 、 Y_B の交換と DHCP とを複合させることによって、パケットの交換回数を増加させずにセッション共有鍵 K の共有を行うことができ、効率的な通信を行うことができる。また、無線端末 8-1 による通信を開始する場合、ハンドオーバを行う場合、および通信が途切れて通信開始時の処理を再び行う場合に、通信確立までの遅延時間の増加を防ぐことができる。無線端末 8-1 およびアクセスポイント 4-1 で共有したセッション共有鍵 K は、無線端末 8-1 とアクセスポイント 4-1 との間の通信において、種々の秘匿および／または認証に使用することができる。なお、

この例では、ハンドオーバーのたびにセッション共有鍵を生成するが、ハンドオーバー先のアクセスポイントが元のアクセスポイントから無線端末のIPやセッション共有鍵を取得するようにしてもよい。

【0071】

つぎに、ローミングを行う場合について説明する。図6は、この実施の形態にかかる、ローミングを行う場合のセッション共有鍵生成処理の処理手順を示す説明図である。ここでは、無線端末9-1およびアクセスポイント4-1がセッション共有鍵Kを生成する場合を例に挙げる。なお、ローミングを行わない場合と同一処理の部分については図5と同一の符号を付している。このセッション共有鍵生成処理では、認証サーバ5-1が、ステップS5で受信したIDが自事業者のIDでないと判定し、このIDに対応する事業者の認証サーバ5-N1に、このIDおよび $E(Y_A)$ を送信して $E(Y_A)$ の復号化を依頼する(S21)。

【0072】

認証サーバ5-N1は、認証サーバ5-1からのIDおよび $E(Y_A)$ を受信すると、このIDに対応する秘密鍵によって $E(Y_A)$ を復号化し、復号化した公開鍵 Y_A を認証サーバ5-1に返信する(S22)。認証サーバ5-1は、認証サーバ5-N1からの公開鍵 Y_A を受信してアクセスポイント4-1に転送する。あるいは、認証サーバ5-N1からアクセスポイント4-1宛てに公開鍵 Y_A を送信してもよい。このように、ローミングを行う場合においても、アクセスポイント4-1および認証サーバ5-1に秘密鍵を知られることなくセッション共有鍵Kの共有を行うことができる。

【0073】

つぎに、DHCPやセッション共有鍵生成処理が終了したあとの、アクセスポイントにおける無線端末の認証処理について説明する。この認証処理では、セッション共有鍵Kを使ってハッシュ値を発生させ、このハッシュ値をMACフレームのCRC値に加味することによってパケット単位の認証を行う。図7は、この実施の形態にかかる無線端末のMACフレーム生成処理の処理手順を示す説明図である。このMACフレーム生成処理において、無線端末は、まず、送信パケットのデータリンク層ペイロードおよびセッション共有鍵Kを含むデータを生成す

る (S 3 1)。

【 0 0 7 4 】

この例では、データリンク層ペイロードをセッション共有鍵Kで挟んだデータを作成するが、データリンク層ペイロードとセッション共有鍵Kの並べ方は特に限定されず、データリンク層ペイロードの片方にセッション共有鍵Kを付加してもよいし、セッション共有鍵Kをデータリンク層ペイロードで挟んでもよい。また、セッション共有鍵Kおよびデータリンク層ペイロードの一部のみを用いてもよい。さらに、このデータにMACヘッダを含めてもよい。つぎに、無線端末は、ステップS 3 1で生成したデータからハッシュ値を算出する (S 3 2)。

【 0 0 7 5 】

つぎに、無線端末は、算出したハッシュ値ならびに送信パケットのMACヘッダおよびデータリンク層ペイロードを含むデータを生成する (S 3 3)。このデータの並べ方も特に限定されない。そして、無線端末は、ステップS 3 3で生成したデータのCRC値を算出し (S 3 4)、このCRC値をMACフレームのCRC値として用い (S 3 5)、このMACフレームをアクセスポイントに送信する。

【 0 0 7 6 】

図 8 は、この実施の形態にかかるアクセスポイントによるパケット単位の認証処理の処理手順を示す説明図である。この認証処理において、アクセスポイントは、まず、無線端末から受信したパケットのデータリンク層ペイロードおよびセッション共有鍵Kを含むデータを、前述した無線端末と同じ方法で生成する (S 4 1)。つぎに、アクセスポイントは、このデータからハッシュ値を算出する (S 4 2) つぎに、アクセスポイントは、算出したハッシュ値ならびに受信パケットのMACヘッダおよびデータリンク層ペイロードを含むデータを、前述した無線端末と同じ方法で生成する (S 4 3)。

【 0 0 7 7 】

そして、アクセスポイントは、ステップS 4 3で生成したデータのCRC値を算出し (S 4 4)、このCRC値と、受信パケットのCRC値とを比較し、これらが同一であれば、このパケットを送信した無線端末が正しいセッション共有鍵

Kを持つ、すなわち、その無線端末が認証サーバと共有する正しい秘密鍵を持つと判断して認証する。このように、パケットフォーマットを変更することなくパケットごとの認証を行うことができるので、データリンクの最大転送可能データ長に影響を与えることがなく、利用者にはトランスピアレントである。

【 0 0 7 8 】

また、この方法は、アクセスポイントから無線端末にパケットを送信する場合にも適用することができる。すなわち、アクセスポイントが前述した無線端末と同じ方法でCRC値を算出してパケットを生成し、無線端末が前述したアクセスポイントと同じ方法でCRC値を算出してパケットごとの認証を行ってもよい。これにより、無線端末側においてパケットごとの認証を行うことができ、アクセスポイントになりすました第3者からのパケットであるかアクセスポイントからの正当なパケットであるかを判定することができる。

【 0 0 7 9 】

つぎに、セッション共有鍵Kを秘匿に用いる場合について説明する。図9は、この実施の形態にかかる秘匿処理を説明する説明図である。ここでは、無線端末8-1とアクセスポイント4-1との通信を例に挙げる。この秘匿処理では、無線端末8-1がアクセスポイント4-1に対してデータパケットを送信する場合、自無線端末が有するセッション共有鍵Kによって該データパケットを暗号化して送信する。暗号化された暗号パケットを受信したアクセスポイント4-1は、自アクセスポイントが有するセッション共有鍵Kによって該暗号パケットを復号化し、宛先に送信する。

【 0 0 8 0 】

また、アクセスポイント4-1が無線端末8-1に対してデータパケットを送信する場合、自アクセスポイントが有するセッション共有鍵Kによって該データパケットを暗号化して送信する。暗号化された暗号パケットを受信した無線端末8-1は、自無線端末が有するセッション共有鍵Kによって該暗号パケットを復号化する。このように、不正な第3者による通信の傍受や発信が容易な無線を介するアクセスポイント4-1と無線端末9-1との通信においても、情報の秘匿を行い、適切な通信を行うことができる。

【0081】

前述した様に、この実施の形態によれば、DHCPに基づいて無線端末側からアクセスポイント側に対して送信されるパケットにセッション共有鍵Kの生成に用いる公開鍵 Y_A を挿入し、DHCPに基づいてアクセスポイント側から無線端末側に対して送信されるパケットにセッション共有鍵Kの生成に用いる公開鍵 Y_B を挿入し、アクセスポイント側で公開鍵 Y_A に基づいてセッション共有鍵Kを生成し、無線端末側で公開鍵 Y_B に基づいてセッション共有鍵Kを生成する。

【0082】

これにより、無線端末とアクセスポイントとの通信を開始する場合のパケット交換回数を増加させることなく、公開鍵 Y_A 、 Y_B の交換を行うことができるため、無線端末とアクセスポイントとの通信確立までの遅延を抑えつつ秘匿用および／または認証用のセッション共有鍵Kを無線端末側およびアクセスポイント側に安全に共有させることができる。また、この実施の形態では、DHCPを例に挙げて説明したが、ARP (Address Resolution Protocol) 等、無線端末－アクセスポイント間の通信に先立って行われる他のプロトコルを用いてもよい。この場合、前述した各DHCP処理部に代えて、そのプロトコルに関する処理を行う処理部を設ける。また、セッション共有鍵に代えて秘密鍵および公開鍵のペアを用いてもよい。

【0083】

【発明の効果】

以上説明したように、この発明のセッション共有鍵共有方法（請求項1）は、第1挿入工程で、無線端末と基地局装置との通信を開始する場合に実行されるプロトコルに基づいて無線端末側から基地局装置側に対して送信されるパケットにセッション共有鍵の生成に用いる第1の情報を挿入し、第2挿入工程で、このプロトコルに基づいて基地局装置側から無線端末側に対して送信されるパケットに、セッション共有鍵の生成に用いる第2の情報を挿入し、第1生成工程で、基地局装置側で第1の情報に基づいてセッション共有鍵を生成し、第2生成工程で、無線端末側で第2の情報に基づいてセッション共有鍵を生成する。これにより、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させる

ことなくセッション共有鍵生成用の情報を交換することができるため、無線端末と基地局装置との通信確立までの遅延を抑えつつ秘匿用および／または認証用のセッション共有鍵を無線端末側および基地局装置側に安全に共有させることができる。

【 0 0 8 4 】

また、この発明のセッション共有鍵共有方法（請求項2）は、ネットワーク層アドレスとMACアドレスとを対応させるプロトコルに基づいて基地局装置側と無線端末側との間で送受信されるパケットにセッション共有鍵生成用の情報を挿入して交換することによって、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させることなくセッション共有鍵生成用の情報を交換することができるため、無線端末と基地局装置との通信確立までの遅延を抑えつつ秘匿用および／または認証用のセッション共有鍵を無線端末側および基地局装置側に安全に共有させることができる。

【 0 0 8 5 】

また、この発明のセッション共有鍵共有方法（請求項3）は、ARPに基づいて基地局装置側と無線端末側との間で送受信されるパケットにセッション共有鍵生成用の情報を挿入して交換することによって、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させることなくセッション共有鍵生成用の情報を交換することができるため、無線端末と基地局装置との通信確立までの遅延を抑えつつ秘匿用および／または認証用のセッション共有鍵を無線端末側および基地局装置側に安全に共有させることができる。

【 0 0 8 6 】

また、この発明のセッション共有鍵共有方法（請求項4）は、ネットワーク層アドレスを無線端末に割り当てるプロトコルに基づいて基地局装置側と無線端末側との間で送受信されるパケットにセッション共有鍵生成用の情報を挿入して交換することによって、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させることなくセッション共有鍵生成用の情報を交換することができるため、無線端末と基地局装置との通信確立までの遅延を抑えつつ秘匿用および／または認証用のセッション共有鍵を無線端末側および基地局装置側に安全

に共有させることができる。

【 0 0 8 7 】

また、この発明のセッション共有鍵共有方法（請求項5）は、DHCPに基づいて基地局装置側と無線端末側との間で送受信されるパケットにセッション共有鍵生成用の情報を挿入して交換することによって、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させることなくセッション共有鍵生成用の情報を交換することができるため、無線端末と基地局装置との通信確立までの遅延を抑えつつ秘匿用および／または認証用のセッション共有鍵を無線端末側および基地局装置側に安全に共有させることができる。

【 0 0 8 8 】

また、この発明の無線端末認証方法（請求項6）は、暗号化工程で、認証に用いるセッション共有鍵の生成用の第1の情報を秘密鍵によって暗号化し、第1挿入工程で、無線端末と基地局装置との通信を開始する場合に実行されるプロトコルに基づいて無線端末側から基地局装置側に対して送信されるパケットに、暗号化工程で暗号化された第1の情報を挿入し、復号化工程で、暗号化された第1の情報を基地局から認証局に送信し、該認証局が復号化した第1の情報を基地局で受信し、第2挿入工程で、このプロトコルに基づいて基地局装置側から無線端末側に対して送信されるパケットに、セッション共有鍵の生成に用いる第2の情報を挿入し、第1生成工程で、復号化工程で復号化された第1の情報に基づいてセッション共有鍵を生成し、第2生成工程で、第2挿入工程で挿入された第2の情報に基づいてセッション共有鍵を生成する。これにより、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させることなく無線端末認証用のセッション共有鍵を無線端末側および基地局装置側に安全に共有させることができるため、無線端末と基地局装置との通信確立までの遅延を抑えつつネットワークに対する不正アクセスを低減することができる。

【 0 0 8 9 】

また、この発明の無線端末認証方法（請求項7）は、ネットワーク層アドレスとMACアドレスとを対応させるプロトコルに基づいて基地局装置側と無線端末側との間で送受信されるパケットにセッション共有鍵生成用の情報を挿入して交

換することによって、無線端末と基地局装置との通信を開始する場合の packets 交換回数を増加させることなく無線端末認証用のセッション共有鍵を無線端末側および基地局装置側に安全に共有させることができるため、無線端末と基地局装置との通信確立までの遅延を抑えつつネットワークに対する不正アクセスを低減することができる。

【0090】

また、この発明の無線端末認証方法（請求項8）は、ARPに基づいて基地局装置側と無線端末側との間で送受信される packets にセッション共有鍵生成用の情報を挿入して交換することによって、無線端末と基地局装置との通信を開始する場合の packets 交換回数を増加させることなく無線端末認証用のセッション共有鍵を無線端末側および基地局装置側に安全に共有させることができるため、無線端末と基地局装置との通信確立までの遅延を抑えつつネットワークに対する不正アクセスを低減することができる。

【0091】

また、この発明の無線端末認証方法（請求項9）は、ネットワーク層アドレスを無線端末に割り当てるプロトコルに基づいて基地局装置側と無線端末側との間で送受信される packets にセッション共有鍵生成用の情報を挿入して交換することによって、無線端末と基地局装置との通信を開始する場合の packets 交換回数を増加させることなく無線端末認証用のセッション共有鍵を無線端末側および基地局装置側に安全に共有させることができるため、無線端末と基地局装置との通信確立までの遅延を抑えつつネットワークに対する不正アクセスを低減することができる。

【0092】

また、この発明の無線端末認証方法（請求項10）は、DHCPに基づいて基地局装置側と無線端末側との間で送受信される packets にセッション共有鍵生成用の情報を挿入して交換することによって、無線端末と基地局装置との通信を開始する場合の packets 交換回数を増加させることなく無線端末認証用のセッション共有鍵を無線端末側および基地局装置側に安全に共有させることができるため、無線端末と基地局装置との通信確立までの遅延を抑えつつネットワークに対す

る不正アクセスを低減することができる。

【0093】

また、この発明の無線端末認証方法（請求項11）は、ディフィーヘルマン型公開鍵配送法を用いてセッション共有鍵を無線端末側および基地局装置側に共有させるため、セッション共有鍵をさらに適切に保護することができる。

【0094】

また、この発明の無線端末認証方法（請求項12）は、第1ハッシュ値算出工程で、無線端末側から基地局装置側に対して送信されるパケットのデータリンク層ペイロードおよび第2生成工程で生成されたセッション共有鍵を含むデータに基づいてハッシュ値を算出し、第1CRC値算出工程で、ペイロードおよび第1ハッシュ値算出工程で算出されたハッシュ値を含むデータに基づいてCRC値を算出し、パケット送信工程で、第1CRC値算出工程で算出されたCRC値をMACヘッダおよびペイロードに付加したパケットを無線端末側から基地局装置側に対して送信し、第2ハッシュ値算出工程で、パケット送信工程で送信されたMACヘッダおよびペイロードならびに第1生成工程で生成されたセッション共有鍵を含むデータに基づいてハッシュ値を算出し、第2CRC値算出工程で、パケット送信工程で送信されたMACヘッダおよびペイロードならびに第2ハッシュ値算出工程で算出されたハッシュ値を含むデータに基づいてCRC値を算出し、認証工程で、パケット送信工程で送信されたCRC値と第2CRC値算出工程で算出されたCRC値とを比較することによって、基地局側で無線端末をパケット単位で認証する。これにより、パケットのフォーマットを変更することなくパケット単位の認証を行うことができるため、さらに適切にネットワークに対する不正アクセスを低減することができる。

【0095】

また、この発明の無線端末（請求項13）は、挿入手段が、基地局装置との通信を開始する場合に実行されるプロトコルに基づいて基地局装置側に対して送信するパケットに、秘匿用および／または認証用のセッション共有鍵の生成に用いる第1の情報を挿入し、取得手段が、このプロトコルに基づいて基地局装置側から送信されるパケットに含まれるセッション共有鍵生成用の第2の情報を取得し

、生成手段が、取得手段が取得した第2の情報に基づいてセッション共有鍵を生成する。これにより、無線端末と基地局装置との通信を開始する場合の packets 交換回数を増加させることなくセッション共有鍵生成用の情報を交換することができるため、無線端末と基地局装置との通信確立までの遅延を抑えつつ秘匿用および／または認証用のセッション共有鍵を無線端末側および基地局装置側に安全に共有させることができる。

【0096】

また、この発明の無線端末（請求項14）は、暗号化手段が、当該無線端末の認証用のセッション共有鍵の生成に用いる第1の情報を秘密鍵によって暗号化し、挿入手段が、基地局装置との通信を開始する場合に実行されるプロトコルに基づいて基地局装置側に対して送信する packets に、暗号化手段が暗号化した第1の情報を挿入し、取得手段が、このプロトコルに基づいて基地局装置側から送信される packets に含まれるセッション共有鍵生成用の第2の情報を取得し、生成手段が、取得手段が取得した第2の情報に基づいてセッション共有鍵を生成する。これにより、無線端末と基地局装置との通信を開始する場合の packets 交換回数を増加させることなく無線端末認証用のセッション共有鍵を無線端末側および基地局装置側に安全に共有させることができるため、無線端末と基地局装置との通信確立までの遅延を抑えつつネットワークに対する不正アクセスを低減することができる。

【0097】

また、この発明の無線端末（請求項15）は、ハッシュ値算出手段が、基地局装置側に対して送信する packets のペイロードおよび生成手段が生成したセッション共有鍵を含むデータに基づいてハッシュ値を算出し、CRC値算出手段が、送信 packets のMACヘッダおよびペイロードならびにハッシュ値算出手段が算出したハッシュ値を含むデータに基づいてCRC値を算出し、パケット送信手段が、CRC値算出手段が算出したCRC値をMACヘッダおよびペイロードに付加した packets を基地局装置側に対して送信する。これにより、packets のフォーマットを変更することなく packets 単位の認証を行うことができるため、さらに適切にネットワークに対する不正アクセスを低減することができる。

【 0 0 9 8 】

また、この発明の基地局装置（請求項 1 6）は、取得手段が、無線端末との通信を開始する場合に実行されるプロトコルに基づいて無線端末側から送信されるパケットに含まれ、秘匿用および／または認証用のセッション共有鍵の生成に用いる第 1 の情報を取得し、挿入手段が、このプロトコルに基づいて無線端末側に対して送信するパケットに、セッション共有鍵の生成に用いる第 2 の情報を挿入し、生成手段が、取得手段が取得した第 1 の情報に基づいてセッション共有鍵を生成する。これにより、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させることなくセッション共有鍵生成用の情報を交換することができるため、無線端末と基地局装置との通信確立までの遅延を抑えつつ秘匿用および／または認証用のセッション共有鍵を無線端末側および基地局装置側に安全に共有させることができる。

【 0 0 9 9 】

また、この発明の基地局装置（請求項 1 7）は、取得手段が、無線端末との通信を開始する場合に実行されるプロトコルに基づいて無線端末側から送信されるパケットに含まれ、秘密鍵によって暗号化された、無線端末の認証用のセッション共有鍵の生成に用いる第 1 の情報を取得し、復号化手段が、取得手段が取得した暗号化された第 1 の情報を、この秘密鍵によって暗号化された情報を復号化して返信する認証局に送信し、該認証局が復号化した第 1 の情報を受信し、挿入手段が、このプロトコルに基づいて無線端末側に対して送信するパケットに、セッション共有鍵の生成に用いる第 2 の情報を挿入し、生成手段が、復号化手段が受信した第 1 の情報に基づいてセッション共有鍵を生成する。これにより、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させることなく無線端末認証用のセッション共有鍵を無線端末側および基地局装置側に安全に共有させることができるため、無線端末と基地局装置との通信確立までの遅延を抑えつつネットワークに対する不正アクセスを低減することができる。

【 0 1 0 0 】

また、この発明の基地局装置（請求項 1 8）は、ハッシュ値算出手段が、無線端末側から受信したパケットのデータリンク層ペイロードおよび生成手段が生成

したセッション共有鍵を含むデータに基づいてハッシュ値を算出し、CRC値算出手段が、このパケットのMACヘッダおよびペイロードならびにハッシュ値算出手段が算出したハッシュ値を含むデータに基づいてCRC値を算出し、認証手段が、無線端末側から受信したパケットのCRC値とCRC値算出手段が算出したCRC値とを比較することによって、無線端末をパケット単位で認証する。これにより、パケットのフォーマットを変更することなくパケット単位の認証を行うことができるため、さらに適切にネットワークに対する不正アクセスを低減することができる。

【図面の簡単な説明】

【図1】

この発明の一実施の形態にかかる通信ネットワークシステムの構成を示す説明図である。

【図2】

図1に示した無線端末の概略構成を示すブロック図である。

【図3】

図1に示したアクセスポイントの概略構成を示すブロック図である。

【図4】

図1に示した認証サーバの概略構成を示すブロック図である。

【図5】

この実施の形態にかかるセッション共有鍵生成処理の処理手順を示す説明図である。

【図6】

この実施の形態にかかる、ローミングを行う場合のセッション共有鍵生成処理の処理手順を示す説明図である。

【図7】

この実施の形態にかかるMACフレーム生成処理の処理手順を示す説明図である。

【図8】

この実施の形態にかかる認証処理の処理手順を示す説明図である。

【図9】

この実施の形態にかかる秘匿処理を説明する説明図である。

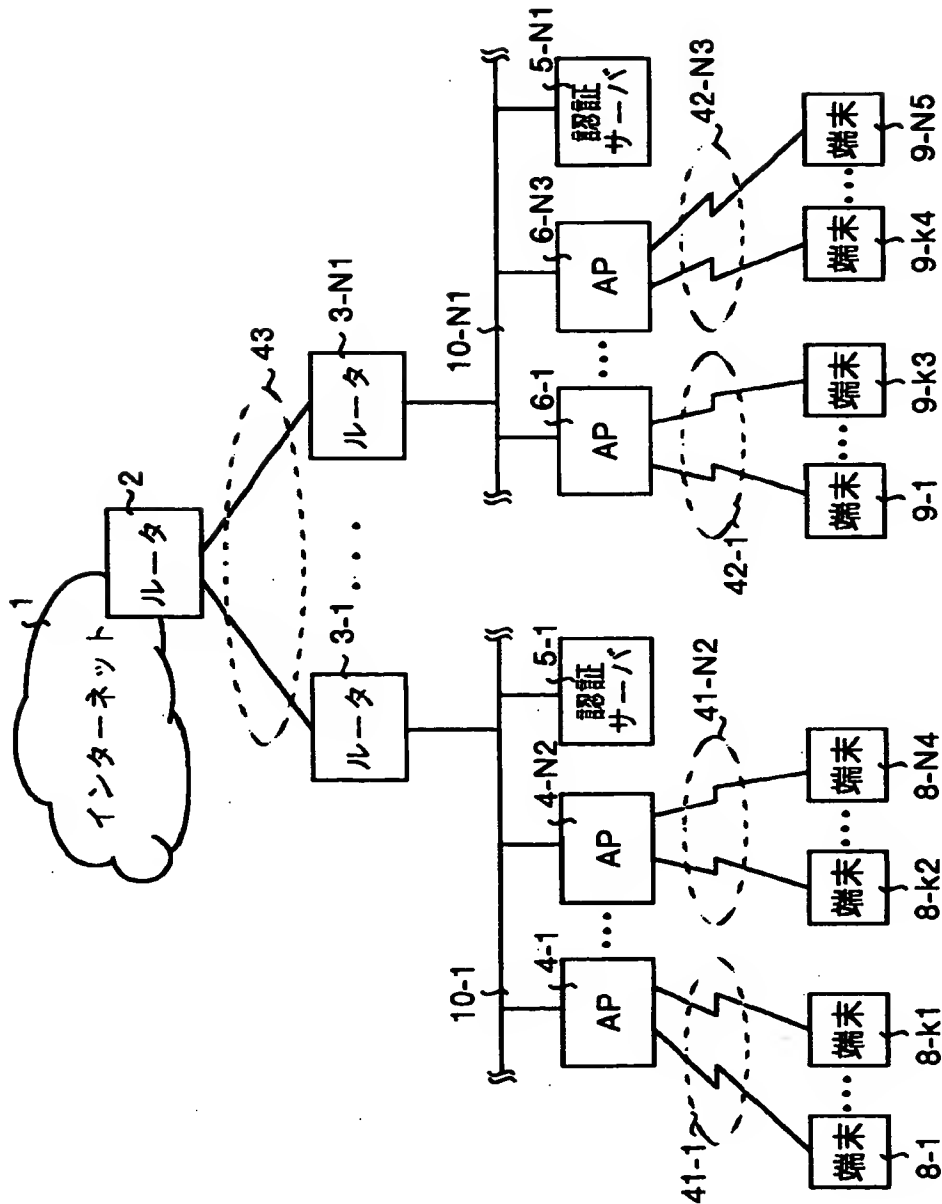
【符号の説明】

- 1 インターネット
- 2, 3-1~3-N1 ルータ
- 4-1~4-N2, 6-1~6-N3 アクセスポイント
- 5-1~5-N1 認証サーバ
- 8-1~8-N4, 9-1~9-N5 無線端末
- 10-1~10-N1 広域LAN
- 11, 22, 31 記憶装置
- 12 ハッシュ値計算部
- 13, 24 ディフィーヘルマン計算部
- 14 CRC値計算部
- 15 暗号化部
- 16, 23, 33 DHCP処理部
- 17, 25 パケット処理部
- 18, 27 無線通信部
- 21, 34 LAN通信部
- 26 ハッシュ値/CRC値計算部
- 28 認証部
- 32 復号化部
- 41-1~41-N2, 42-1~42-N3 無線ネットワーク
- 43 バックボーンネットワーク

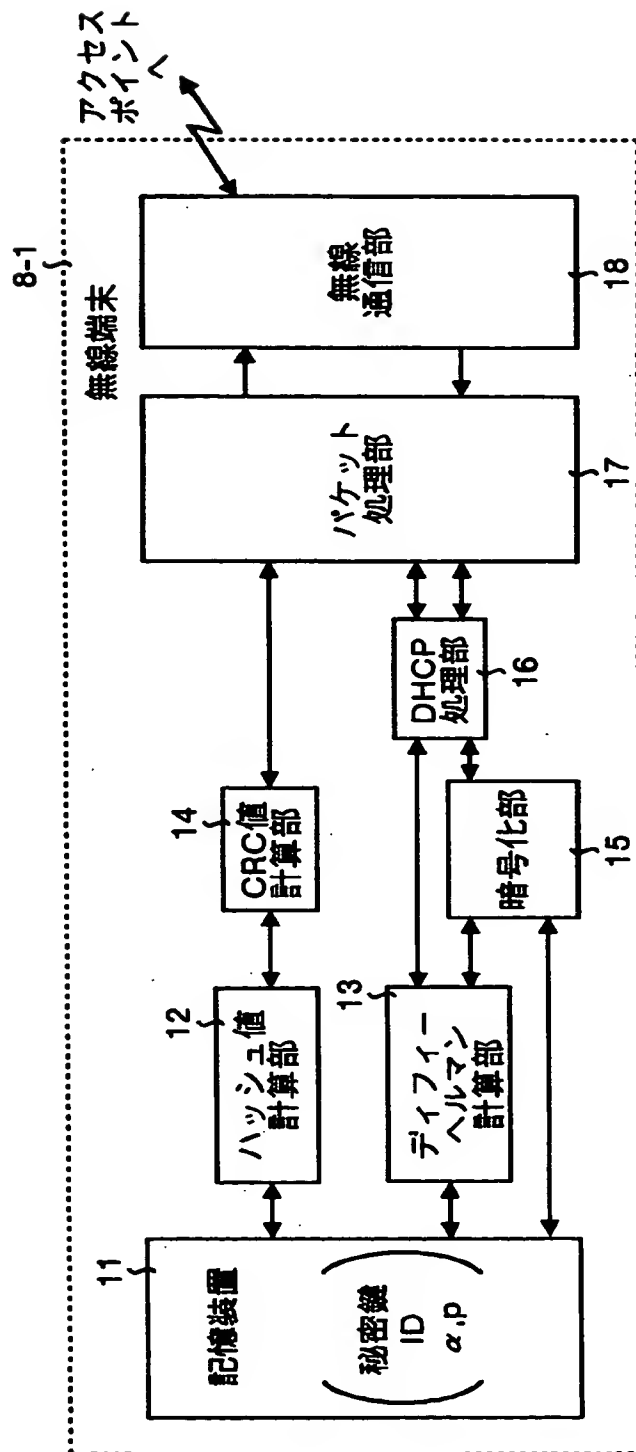
【書類名】

図面

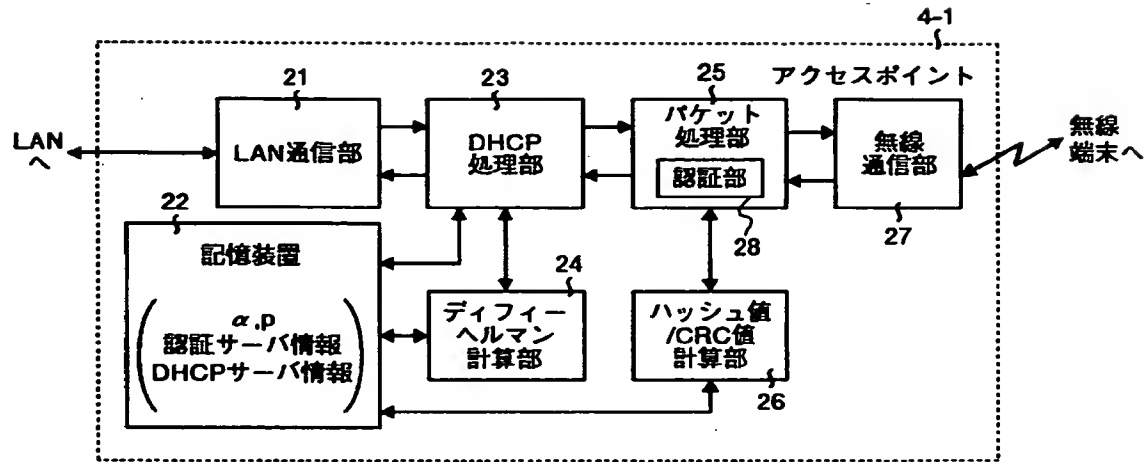
【図 1】



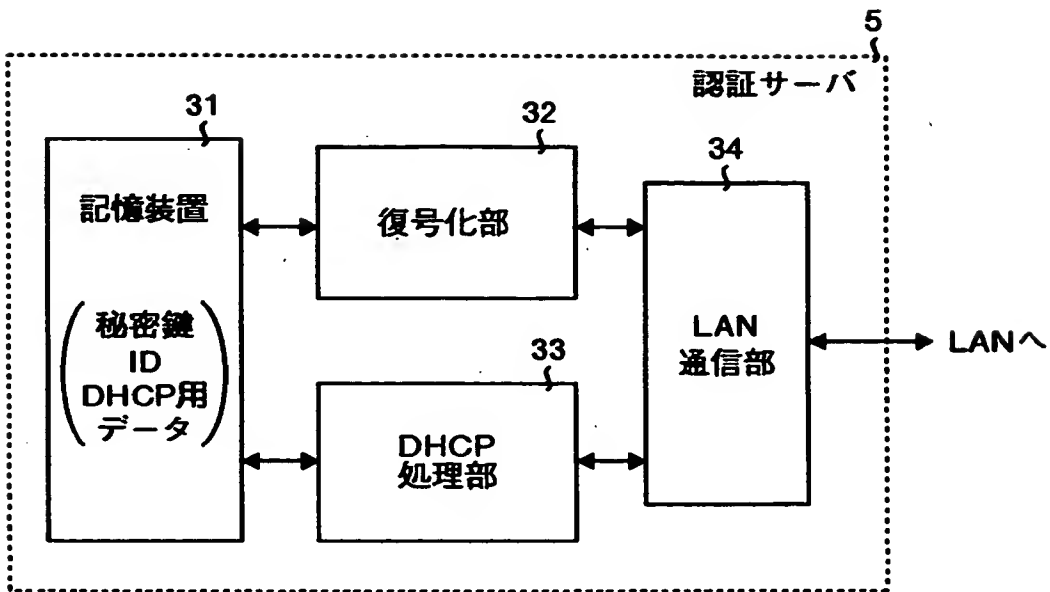
【図 2】



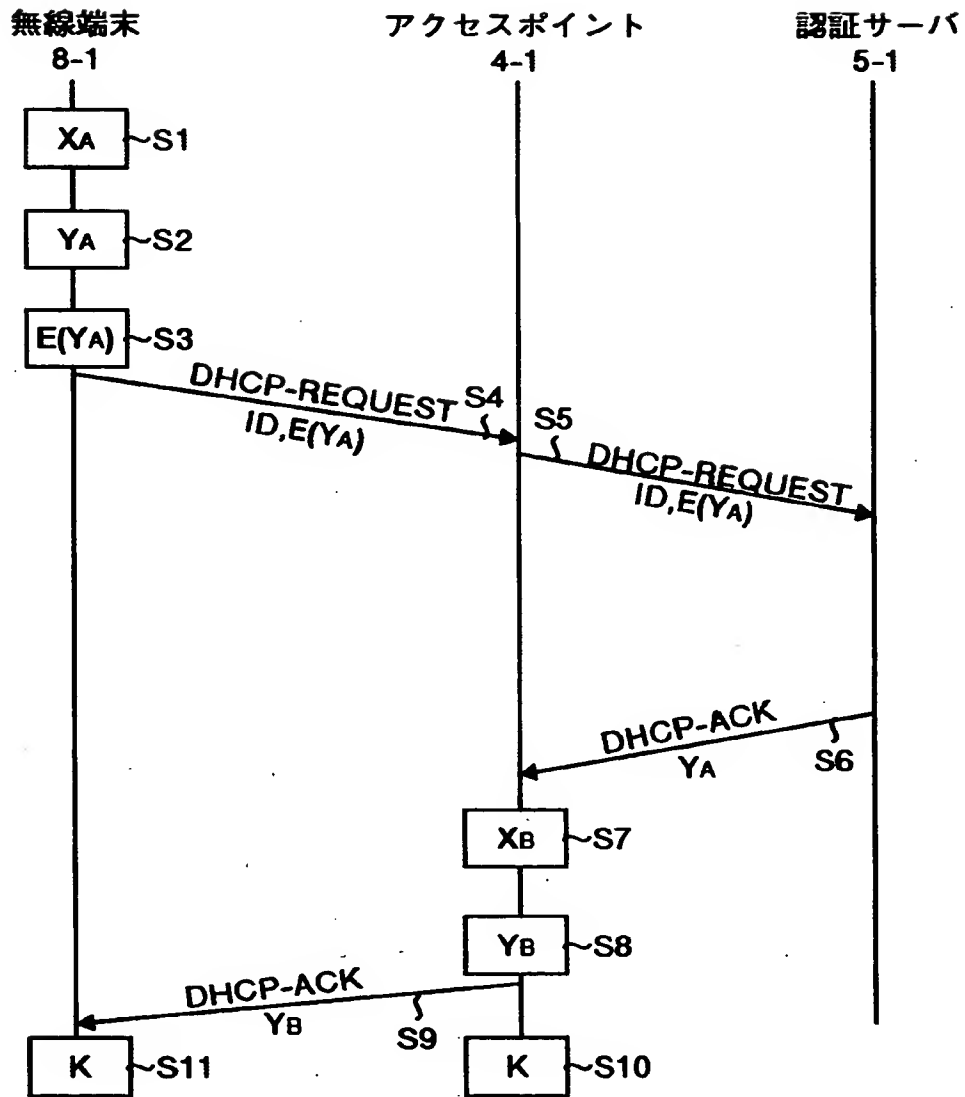
【図 3】



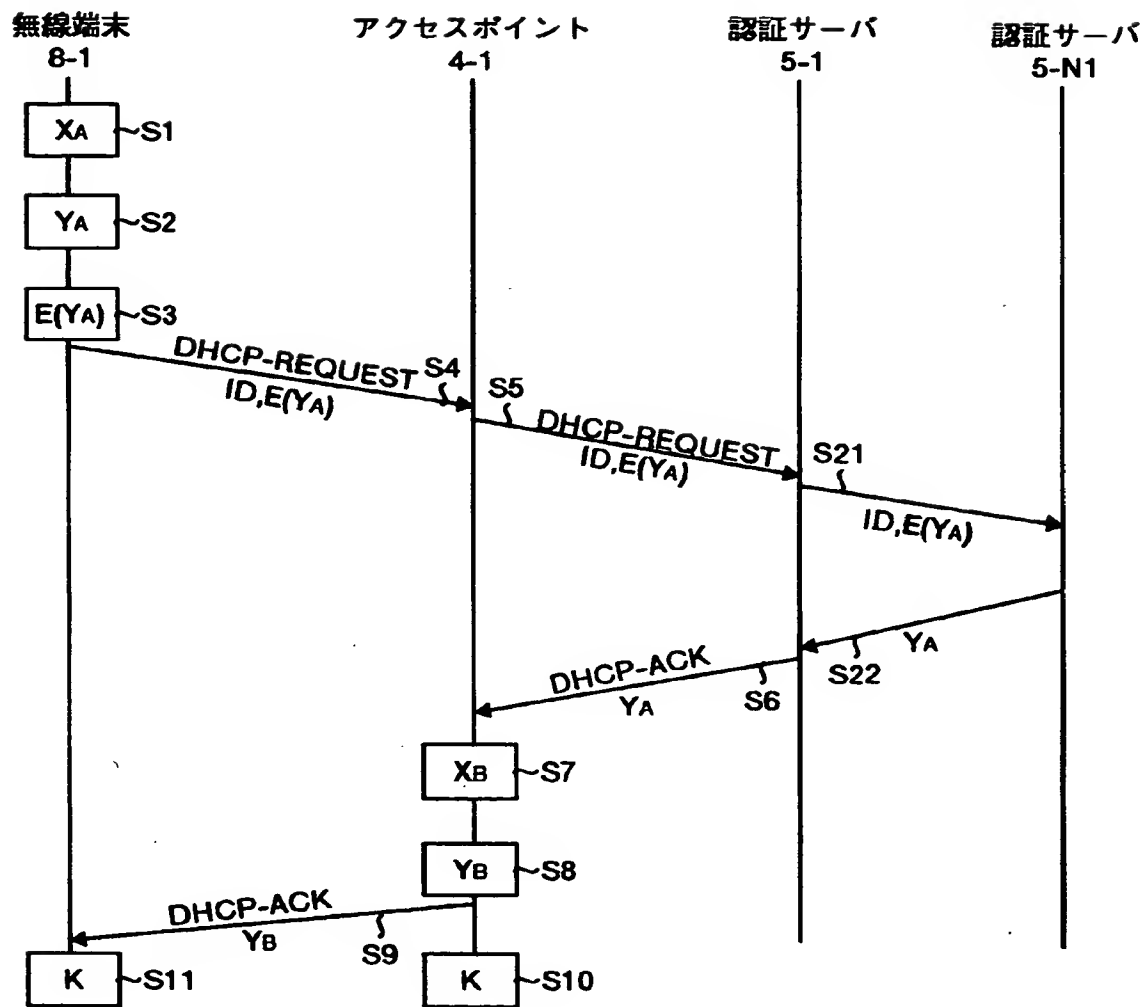
【図 4】



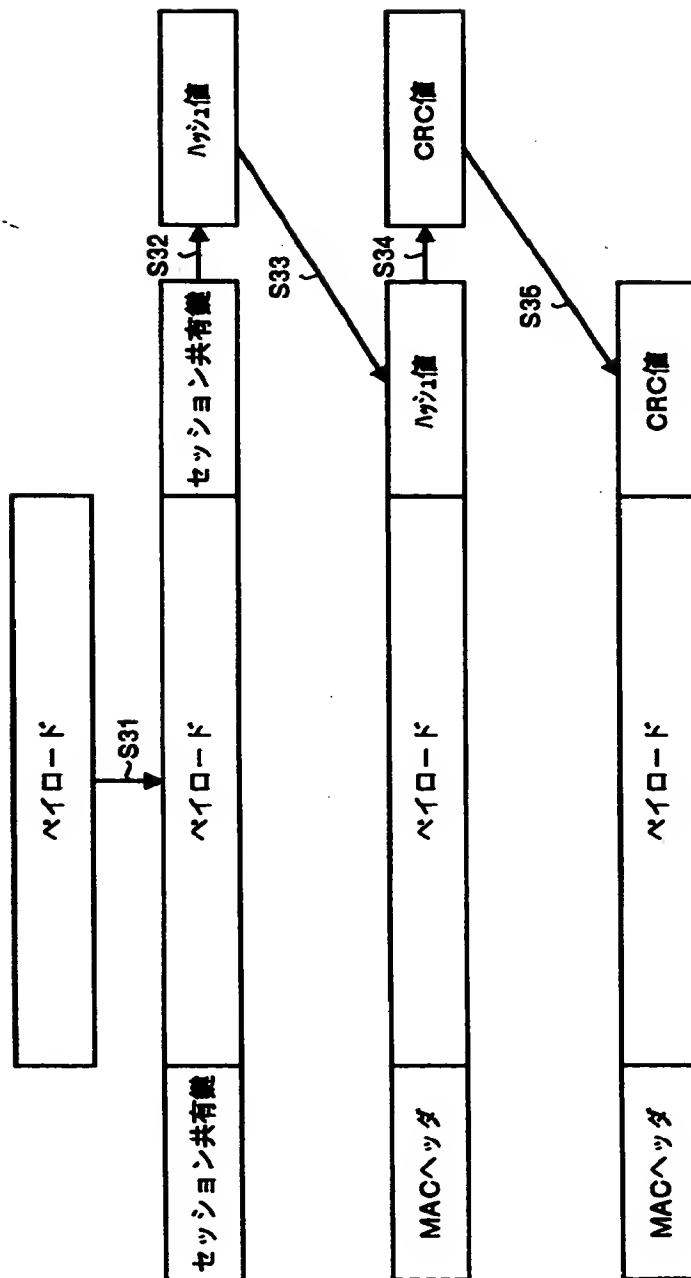
【図 5】



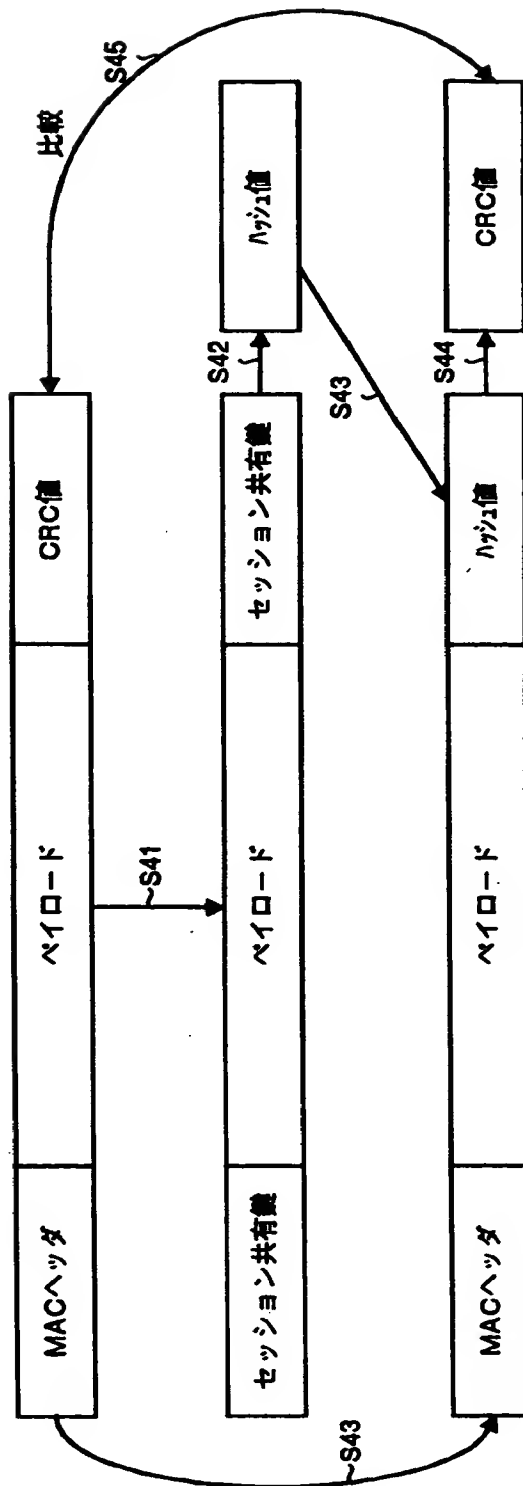
【図 6】



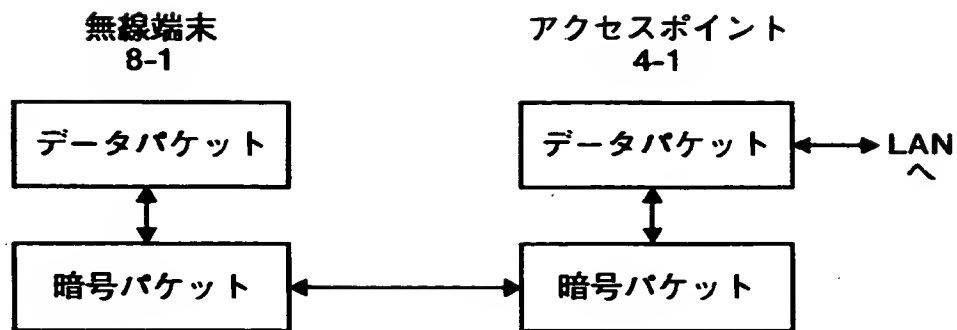
【図 7】



【図 8】



【図 9】



【書類名】 要約書

【要約】

【課題】 無線端末とアクセスポイントとの通信確立までの遅延を抑えつつ秘匿用および／または認証用のセッション共有鍵 K を無線端末側およびアクセスポイント側に安全に共有させること。

【解決手段】 $DHCP$ に基づいて無線端末 8-1 側からアクセスポイント 4-1 側に対して送信されるパケットにセッション共有鍵 K の生成に用いる公開鍵 Y_A を挿入し、 $DHCP$ に基づいてアクセスポイント 4-1 側から無線端末 8-1 側に対して送信されるパケットにセッション共有鍵 K の生成に用いる公開鍵 Y_B を挿入し、アクセスポイント 4-1 側で公開鍵 Y_A に基づいてセッション共有鍵 K を生成し、無線端末 8-1 側で公開鍵 Y_B に基づいてセッション共有鍵 K を生成する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000005290]

1. 変更年月日	1990年 8月29日
[変更理由]	新規登録
住 所	東京都千代田区丸の内2丁目6番1号
氏 名	古河電気工業株式会社